4N

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,305	07/13/2001	Maximilian Luttrell	PV01-108-US1	6355

25209 7590 03/08/2005

PACKETVIDEO CORPORATION
4820 EASTGATE MALL
SAN DIEGO, CA 92121

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,305	LUTTRELL ET AL.	
	Examiner	Art Unit	
	Brandon S Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-11 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-11 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 13 July 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP §608.01.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Isnardi (U.S. Patent No. 6,687,384) in view of Thompson, Jr. et al. (U.S. Patent No. 5,978,483).

Regarding claim 1, Isnardi teaches a method for access control of a standard compliant multimedia bitstream comprising:

- Selectively extracting codewords from the bitstream (col. 7, lines 31-67 and fig. 4);
- Encrypting the extracted codewords (col. 8, lines 1-15 and fig. 5); and

- Mapping the encrypted codewords back into the bitstream (col. 8, lines 16-67 and fig. 6),
- Wherein the resulting encrypted bitstream is a secure bitstream accessible by users with a proper key (col. 9, lines 1-46 and fig. 7), and has a number of codewords equal to the number of codewords in the bitstream prior to encryption to maintain standard compliance (col. 4, lines 15-20).

Isnardi does not specifically teach encryption with the use of keys, but data hiding and watermarking instead.

Thompson, Jr. et al. teaches encryption with keys (col. 3, line 53 through col. 4, line 2).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine encryption with keys, as taught by Thompson, Jr. et al., with the method of Isnardi. It would have been obvious for such modifications because Isnardi discusses using either encryption (for preventive purposes) or watermarking (for identifying purposes). Both methods are used for defensive purposes (see col. 1, lines 22-32 of Isnardi). Thompson, Jr. et al. further elaborates on the encryption method.

Regarding claim 2, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the bitstream has an associated standard defined code table (see

Table III and Table V of Thompson, Jr. et al.), the codewords each have an assigned fixed length index and the step of encrypting comprises: concatenating the extracted codewords to form a codeword concatenation C; mapping the concatenated codewords to indices in the code table; concatenating the mapped indices to provide a binary bit string S; encrypting the binary bit string S with a chosen secure cipher to provide an encrypted binary bit string S^1; and mapping S^1 to codewords in the code table to form an encrypted codeword concatenation C^1 (see fig. 2 and col. 3, line 53 through col. 4, line 2 and col. 5, line 54 through col. 6, line 32 of Thompson, Jr. et al.). Isnardi teaches MPEG data, which is known to have codewords. Isnardi alone extracts portions of the codewords for data hiding. The combination with Thompson, Jr. et al. would encrypt the codewords.

Regarding claim 3, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the bitstream has a syntax comprising multiple information fields, and the step of selectively extracting codewords comprises extracting variable length codewords from a particular information field (see col. 7, lines 36-49 of Isnardi).

Regarding claim 4, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the bitstream is an MPEG-4 error resilient, data partitioned bitstream, and the step of selectively extracting codewords comprises extracting motion vector information from the bitstream (see col. 7, lines 36-49 of Isnardi).

Regarding claim 5, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the bitstream is an MPEG-4 video bitstream, and the step of selectively extracting codewords comprises extracting fixed length coded texture information (see col. 4, lines 3-4 of Isnardi, FLC is used in MPEG standards as discussed by Isnardi).

Regarding claim 6, Thompson, Jr. et al. teaches a compliance preserving encryption method for a concatenated sequence of variable length code (VLC) codewords, the method comprising: mapping each VLC codeword to a fixed length index in a code table to obtain a concatenation of fixed length indices; encrypting the concatenation of fixed length indices with a chosen cipher; and mapping the encrypted concatenation of indices to VLC codewords in the code table to obtain an encrypted concatenation of VLC codewords (fig. 2 and col. 3, line 53 through col. 4, line 2 and col. 5, line 54 through col. 6, line 32).

Thompson, Jr. et al. does not teach wherein the number of codewords in the concatenated sequence remains unchanged before and after encryption such that syntax compliance is maintained.

Isnardi teaches wherein the number of codewords in the concatenated sequence remains unchanged before and after encryption such that syntax compliance is maintained (col. 4, lines 15-20).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the number of codewords in the concatenated sequence remains unchanged before and after encryption such that syntax compliance is maintained, as taught by Isnardi, with the method of Thompson, Jr. et al. It would have been obvious for such modifications because maintaining the correct number of codewords after encryption provides a secure stream that is still MPEG compliant (see col. 4, lines 15-20 of Isnardi). This means a standard MPEG decoder can act upon the stream. Isnardi teaches MPEG data, which is known to have codewords. Isnardi alone extracts portions of the codewords for data hiding. The combination with Thompson, Jr. et al. would encrypt the codewords.

Regarding claim 7, Isnardi teaches a system for access control of a standardized multimedia partitioned bitstream comprising:

- An encoder capable of scrambling header information in the partitioned bitstream and remapping the scrambled information into a standard compliant header partition resulting in an encrypted bitstream (col. 8, lines 1-67 and fig. 5/6); and
- A decoder having a decryption key capable of recovering proper header information (col. 9, lines 1-46 and fig. 7),
- Wherein the bitstream can be transmitted over an error prone channel and recovered for correct interpretation by an authorized end user (col. 4, lines 15-20).

Isnardi does not specifically teach scrambling with the use of keys, but data hiding instead.

Thompson, Jr. et al. teaches scrambling with keys (col. 3, line 53 through col. 4, line 2).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine scrambling with keys, as taught by Thompson, Jr. et al., with the method of Isnardi. It would have been obvious for such modifications because Isnardi discusses using either encryption (for preventive purposes) or watermarking (for identifying purposes). Both methods are used for defensive purposes (see col. 1, lines 22-32 of Isnardi). Thompson, Jr. et al. further elaborates on the encryption method.

Regarding claim 8, Isnardi teaches a method for access control of a multimedia bitstream, the method comprising steps of:

- Accessing a portion of the bitstream to extract selective information (col. 7, lines 31-67 and fig. 4);
- Scrambling the extracted selective information to provide encrypted codewords (col. 8, lines 1-15 and fig. 5); and
- Mapping the encrypted codewords back into the portion of the bitstream (col. 8, lines 16-67 and fig. 6),

- Wherein the resulting bitstream is a secure bitstream accessible by users with a proper key (col. 9, lines 1-46 and fig. 7).

Isnardi does not specifically teach scrambling with the use of a key, but data hiding instead.

Thompson, Jr. et al. teaches scrambling with the use of a key (col. 3, line 53 through col. 4, line 2).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine scrambling with the use of a key, as taught by Thompson, Jr. et al., with the method of Isnardi. It would have been obvious for such modifications because Isnardi discusses using either encryption (for preventive purposes) or watermarking (for identifying purposes). Both methods are used for defensive purposes (see col. 1, lines 22-32 of Isnardi). Thompson, Jr. et al. further elaborates on the encryption method.

Regarding claim 9, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the bitstream is a standardized data partitioned bitstream, and wherein the step of accessing comprises accessing a header portion of the bitstream having coding type information and motion vector information (MV codewords), and extracting the MV codewords (see col. 7, lines 36-49 of Isnardi).

Regarding claim 10, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the scrambling step comprises: mapping the extracted MV codewords to indices of a standard MV code table for the bitstream; concatenating the mapped indices to provide a binary bit string S; encrypting the binary bit string S to provide an encrypted binary bit string S'; dividing the encrypted binary bit string S' into equal length segments; using the equal length codewords to index the standard MV code table to construct a sequence of new MV codewords; and entropy encoding the new MV codewords (see fig. 2 and col. 3, line 53 through col. 4, line 2 and col. 5, line 54 through col. 6, line 32 of Thompson, Jr. et al.). Isnardi teaches MPEG data, which is known to have Motion Vector codewords. Isnardi alone extracts portions of the codewords for data hiding. The combination with Thompson, Jr. et al. would encrypt the codewords.

Regarding claim 11, the combination of Isnardi in view of Thompson, Jr. et al. teaches wherein the bitstream is an MPEG-4 video bitstream and wherein the extracted selective information is fixed length code (FLC) texture information (see col. 4, lines 3-4 of Isnardi, FLC is used in MPEG standards as discussed by Isnardi).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BH

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100